

RECEIVED
CENTRAL FAX CENTER

001/008



MAY 26 2006

Western Digital Corporation
20511 Lake Forest Drive, E118-G
Lake Forest, California 92630Tel: 949.672.7000
Fax: 949.672.6604

TO:	COMMISSIONER FOR PATENTS, U.S. PATENT & TRADEMARK OFFICE		
FAX NO:	(571) 273-8300 (GENERAL/MAIN FAX LINE)		
NO. OF PAGES:	Cover + 7		
CERTIFICATE OF FACSIMILE TRANSMISSION I hereby certify that this correspondence is being facsimile transmitted to the U.S. Patent and Trademark Office on the date indicated below.		APPLICATION NO.	09/608,103
<u>Renee M. Franks</u> Typed/Printed Name		FILING DATE	06/30/2000
<u></u> Signature		FIRST NAMED INVENTOR	Christopher L. Hamlin
<u>May 26, 2006</u> Date		ART UNIT	2136
		CONFIRMATION NO.	1085
		EXAMINER	Carl G. Colin
		ATTORNEY DOCKET NO.	K35A0631
TITLE	SECURE DISK DRIVE COMPRISING A SECURE DRIVE KEY AND A DRIVE ID FOR IMPLEMENTING SECURE COMMUNICATION OVER A PUBLIC NETWORK		

ATTACHED WITH THIS SUBMISSION:

1. Notice of Appeal (1 page)
2. Pre-Appeal Brief Request for Review (1 page)
3. Reasons for Pre-Appeal Brief Review (5 pages)

PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION. IF THERE IS ANY PROBLEM WITH THIS TRANSMISSION, PLEASE CALL RENEE M. FRANKS AT (949) 672-7871.

CONFIDENTIALITY NOTE

THE INFORMATION CONTAINED IN THIS FACSIMILE TRANSMISSION MAY BE LEGALLY PRIVILEGED AND IS CONFIDENTIAL INFORMATION INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY NAMED ABOVE. IT IS EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAW, INCLUDING COURT ORDERS, IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT OR THE EMPLOYEE OR AGENT RESPONSIBLE FOR DELIVERING THIS FACSIMILE TRANSMISSION TO THE INTENDED RECIPIENT. YOU ARE HEREBY NOTIFIED THAT ANY USE, DISSEMINATION, DISTRIBUTION OR COPY OF THIS FACSIMILE TRANSMISSION OR ITS INFORMATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS FACSIMILE TRANSMISSION IN ERROR, PLEASE IMMEDIATELY NOTIFY US BY TELEFAX OR TELEPHONE USING THE ABOVE NUMBERS AND AIRMAIL THIS FACSIMILE TRANSMISSION BACK TO US IMMEDIATELY. THANK YOU.

Y:\UP\PROGRAM\ICSA\FILES\VA0600-A0699\A0631\PTO\A0631_Faxcover USPTO - GENERAL.doc

2006 05/26 FRI 14:37 FAX 949 672 6626

RECEIVED
CENTRAL FAX CENTER

003/008

MAY 26 2006

Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)

Approved for use through 10/22/200x. OMB 0651-00xx

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)

K35A0631

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" (37 CFR 1.8(a))

on _____

Signature_____

Typed or printed name _____

Application Number

09/608,103

Filed

06/30/2000

First Named Inventor

Christopher L. Hamlin

Art Unit

2136

Examiner

Carl G. Colin

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).

Note: No more than five (5) pages may be provided.

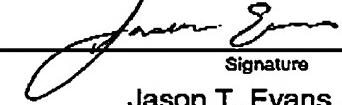
I am the

applicant/inventor.

assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

attorney or agent of record.

Registration number 57,862.


Signature

Jason T. Evans, Esq.

Typed or printed name

(949) 672-9474

Telephone number

attorney or agent acting under 37 CFR 1.34.

Registration number if acting under 37 CFR 1.34 _____

May 26, 2006

Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below.



*Total of One (1) forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

RECEIVED
CENTRAL FAX CENTER

MAY 26 2006

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appn. of:	Christopher L. Hamlin	Art Unit:	2136
Serial No.:	09/608,103	Examiner:	Carl G. Colin
Filing Date:	06/30/2000	Confirmation No.:	1085
For: SECURE DISK DRIVE COMPRISING A SECURE DRIVE KEY AND A DRIVE ID FOR IMPLEMENTING SECURE COMMUNICATION OVER A PUBLIC NETWORK		Docket No.:	K35A0631

REASONS FOR PRE-APPEAL BRIEF REVIEW

MAIL STOP AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Dear Sir,

The following reasons are submitted for a pre-appeal brief review together with a Notice of Appeal filed herewith for the above-identified application.

SUMMARY OF CLAIMED SUBJECT MATTER

FIG. 2 shows a secure disk drive 20 according to an embodiment of the present invention as comprising a disk 22 for storing data, and an input 24 for receiving an encrypted message 26 from a client disk drive, the encrypted message 26 comprising ciphertext data and a client drive ID identifying the client disk drive. The secure disk drive 20 comprises a secure drive key 34 and an internal drive ID 38. A key generator

Art Unit 2136
Serial No.: 09/608,103

Reply to Office Action of: 04/05/2006
Attorney Docket No.: K35A0631

30 within the secure disk drive 20 generates a client drive key 32 based on the client drive ID and the secure drive key 34, and an internal drive key 36 based on the internal drive ID 38 and the secure drive key 34. The secure disk drive 20 further comprises an authenticator 56 for verifying the authenticity of the encrypted message 26 and generating an enable signal 50, the authenticator 56 is responsive to the encrypted message 26 and the client drive key 32. The secure disk drive further comprises a data processor 40 comprising a message input 42 for receiving the encrypted message 26 from the client disk drive, and a data output 58 for outputting the ciphertext data 46 to be written to the disk 22. The data processor 40 further comprises an enable input 48 for receiving the enable signal 50 for enabling the data processor 40, and a key input 51 for receiving the internal drive key 36, the internal drive key 36 for use in generating a message authentication code. The data processor 40 outputs reply data 54 comprising the message authentication code. The secure disk drive 20 outputs a reply 60 to the client disk drive, the reply 60 comprising the reply data 54 and the internal drive ID 38.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-16 stand rejected under 35 USC §103(a) as unpatentable over U.S. Patent No. 6,226,750 to Trieger in view of U.S. Patent No. 6,473,861 to Stokes and in view of U.S. Patent No. 5,931,947 to Burns et al..

The examiner asserts that Trieger discloses a secure disk drive for receiving an encrypted message from a client disk drive, the encrypted message comprising ciphertext data and a device ID identifying the client disk drive. The examiner further asserts that Trieger discloses a secure disk drive that generates a client drive key based on the client drive ID and a secure drive key (state information) for use in authenticating the client drive ID. The applicant respectfully disagrees.

Art Unit 2136
Serial No.: 09/608,103

Reply to Office Action of: 04/05/2006
Attorney Docket No.: K35A0631

ARGUMENT

I. THE ISSUE UNDER 35 U.S.C. §103(a)

- A. The rejection should be reversed because the state information disclosed by Trieger is not a secure drive key

The examiner asserts that Trieger discloses a secure disk drive that generates a client drive key based on the client drive ID and a secure drive key (state information) for use in authenticating the client drive ID. However, the state information disclosed by Trieger merely refers to information associated with a particular communication session between a client and a server. The server saves the state information so that the client does not have to resend the state information with each new communication request (see col. 9, lines 20-27). The state information cannot be considered a secure drive key because a client drive key is not generated based on the state information, with an authenticator responsive to the generated client drive key, as recited in the claims.

In Trieger, a server initially authenticates a client by the client sending authentication information, such as a password, to the server (see col. 7, line 65 to col. 8, line 12). If the authentication information is approved, the server generates a first key that identifies the client (device ID), and transmits the key to the client (col. 8, lines 12-15). During a subsequent communication session, the server authenticates the client by validating the key (device ID) sent to the server in a communication request (see col. 8, lines 63-66). As described at col. 9, lines 4-9, Trieger teaches to validate the key by "comparing the value of key 92 with key values stored in a key storage database at the server 52....[or] the key may be self-validating in that the server 52 may be able to immediately recognize the key's information or format." Nowhere does Trieger (or the other relied upon prior art, alone or in combination) disclose or suggest that, when an encrypted message including a client drive ID is received, an authenticator verifies the authenticity of the encrypted message responsive to a client drive key generated based on the client drive ID and a secure drive key.

The examiner also asserts that Burns discloses a reply that may contain an internal drive ID so that devices can authenticate each other. This interpretation of Burns is incorrect. Burns discloses a secure disk drive for authenticating messages

Art Unit 2136
Serial No.: 09/608,103

Reply to Office Action of: 04/05/2006
Attorney Docket No.: K35A0631

received from a client user or subscriber and does not disclose devices authenticating each other. (See Abstract, wherein "all encryption is done by the clients, rather than by the devices.") As discussed by the applicant in the specification at page 4, lines 4-6, in Burns, "the keys used by the clients for encrypting data and generating the message authentication codes are generated external to the devices by a system administrator which is susceptible to attack."

In the final office action, the examiner asserts that Burns discloses (col. 3, line 65 through col. 4, line 7) "the network storage devices can be comprised of existing direct access disk devices and files can be copied directly from one storage device to another in a secure manner, the networks clients only involvement would be to initiate the action." However, this does not mean that the storage devices authenticate one another, it merely means that files can be safely copied from one storage device to another because the files have already been encrypted by the clients. In any event, the examiner concedes it is the network clients that "initiate the action", which means the request to transfer files comes from a network client and not another storage device. In Burns, it is the requests generated by the network clients that are authenticated by the storage device and not requests generated by other storage devices.

Art Unit 2136
Serial No.: 09/608,103

Reply to Office Action of: 04/05/2006
Attorney Docket No.: K35A0631

CONCLUSION

Reversal of the rejections is respectfully requested.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 23-1209, and please credit any excess fees to such deposit account.

Respectfully submitted,

Date: May 26, 2006

By: 

Jason T. Evans, Esq.
Reg. No. 57,862

WESTERN DIGITAL TECHNOLOGIES, INC.
20511 Lake Forest Drive
Lake Forest, CA 92630
Tel.: (949) 672-7000
Fax: (949) 672-6604